UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA

MALINDA S. SMIDGA, individually and on behalf of all others similarly situated, Plaintiff, v. META PLATFORMS, INC. f/k/a FACEBOOK, INC., THE UNIVERSITY OF PITTSBURGH MEDICAL CENTER d/b/a UPMC, Defendants.	Case No. 2:22-cv-1231 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Malinda S. Smidga ("Plaintiff"), on behalf of herself and all others similarly situated, asserts the following against Defendants Meta Platforms, Inc. f/k/a Facebook, Inc ("Meta") and University Pittsburgh Medical Center d/b/a UPMC ("UPMC") (collectively, "Defendants"), based upon personal knowledge, where applicable, information and belief, and the investigation of counsel.

SUMMARY OF ALLEGATIONS

1. In 2004, Mark Zuckerberg launched TheFacebook.com as a directory and social network for Harvard students.[1] Meta has since grown exponentially, becoming one of the largest advertising companies in the country.

[1] Alan Taback, *Hundreds Register for New Facebook Website* (Feb. 9, 2004), https://www.thecrimson.com/article/2004/2/9/hundreds-register-for-new-facebook-website/.

2. In 2021, Meta generated more than 97% of its total revenue from advertising, with $114.93 billion reported in advertising revenue.[2]

3. To operate its advertising enterprise, Meta relies on tracking tools like the "Meta Pixel."

4. Meta Pixel is a snippet of JavaScript code embedded on a third-party website that tracks users' actions as they navigate through the website. It logs the pages they visit, the buttons they click, the information they type, and more.[3] Meta Pixel then sends this harvested information to Meta, where it can be stored for years.[4]

5. Meta surreptitiously profits from this large-scale data collection. When the Meta Pixel is embedded in a third-party website, and without users' knowledge or consent, Meta is able to gather every user interaction with that site. Meta then aggregates this data across all websites in order to build a dossier of that user's activity, labeled with the user's IP address, and matched to the user's Facebook and/or Instagram account (or lack thereof).[5]

6. The Meta Pixel is marketed towards third parties that use Facebook Ads as a way to "make sure [their] ads are shown to the right people." Meta boasts that Meta Pixel allows third

---

[2] Meta Investor Relations, *Meta Reports Fourth Quarter and Full Year 2021 Results* (Feb. 2, 2022), https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx.

[3] Todd Feathers, Simon Fondrie-Teitler, Angie Waller, & Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, The Markup (June 16, 2022) ("Feathers et al."), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

[4] Facebook Business Tools Terms, https://m.facebook.com/legal/terms/businesstools, (last visited Aug. 25, 2022).

[5] *Id.*

parties to improve users experience on their websites, target advertisements more effectively, and drive more sales.[6]

7. These benefits appeal to third-party websites; 30% of the 100,000 most popular websites use Meta Pixel, and Meta has reported that millions of iterations of its Pixel are on websites across the Internet.[7] Those websites include those operated by healthcare service entities that store and convey sensitive, private health information.[8]

8. Recently, it was discovered that the Meta Pixel is embedded on the websites of one-third of the top 100 U.S. hospitals and, more egregiously, on the password-protected patient portals of seven health systems.[9] Notably, it was found on UPMC's appointment scheduling page.

9. When a user enters sensitive health and personal information on UPMC's appointment scheduling page, the Meta Pixel then sends some of that data to Meta.

10. The data can include a user's medical condition, prescriptions, appointments, test results, diagnoses, allergies, sexual orientation, treatment status, reason for requesting an appointment, and more. As with other types of data collected by Meta Pixel, this sensitive information is sent to Meta along with the user's IP address (an IP address is an identifier that is similar to a computer's mailing address and can generally be linked to a specific individual or household). Additionally, if a user is logged in to Facebook when they visit a hospital website in which Meta Pixel is embedded, Meta may link their private information to their Facebook account.

---

[6] Meta Business Help Center, *About Meta Pixel*, https://www.facebook.com/business/help/742478679120153?id=1205376682832142, (last visited Aug. 25, 2022).

[7] The Markup, *How We Built a Meta Pixel Inspector* (Apr. 28, 2022), https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector.

[8] Feathers et al., *supra* note 3.

[9] *Id.*

11. Meta monetizes the information it receives through Meta Pixel by using it to generate highly profitable targeted advertising; the type of advertising on which it relies for the majority of its revenue.

12. The targeted advertising Meta offers for sale includes the ability to target patients based on specific sensitive health information that a patient has provided on UPMC's appointment scheduling page.

13. Plaintiff had her sensitive health information harvested by Meta through the Meta Pixel without her knowledge or consent when she entered her information on UPMC's appointment scheduling page.

14. As a result of Meta's illegal data harvesting, Plaintiff began to receive targeted advertisements that were specifically related to the medical information that she thought was secure on UPMC's website.

15. Both Meta and UPMC recklessly disregarded patient privacy in order to maximize their own profits.

16. Defendants' actions constitute an extreme invasion of Plaintiff's and Class members' right to privacy and violate federal and state statutory and common law.

PARTIES

17. Plaintiff Malinda S. Smidga is a resident of Allegheny County, Pennsylvania. Plaintiff is a citizen of Pennsylvania.

18. Plaintiff is a Facebook user and has had a Facebook account since approximately 2010.

19. Plaintiff was a patient of UPMC and has used UPMC's appointment scheduling page since approximately 2014.

20. To make appointments, and research and communicate with her doctors, Plaintiff was advised to utilize the UPMC website.

21. Plaintiff's use of the appointment scheduling page entailed entering her personal information, as well as sensitive medical information to dictate the reason for her visit to UPMC.

22. Meta surreptitiously collected this data and associated it with Plaintiff's Facebook account for use in targeting her with advertisements.

23. Indeed, after entering this information on UPMC's appointment scheduling page, Plaintiff received advertisements on her Facebook page targeted to her symptoms.

24. Defendant UPMC is an integrated global health enterprise, and one of the leading nonprofit healthcare systems in the United States. UPMC is comprised of 40 hospitals and 800 doctors' offices and outpatient sites. UPMC serves the healthcare needs of approximately 4 million people per year.

25. Defendant UPMC is a public nonprofit educational institution and is headquartered at 200 Lothrop Street, Pittsburgh, Pennsylvania 15213. UPMC is a citizen of Pennsylvania.

26. Defendant Meta (f/k/a Facebook, Inc.) is a publicly traded Delaware corporation headquartered in Menlo Park, California, which does business throughout the United States and the world, deriving significant revenue from interstate commerce. Meta is a citizen of California.

JURISDICTION AND VENUE

27. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C § 1332(d), because the amount in controversy for the Class exceeds $5,000,000 exclusive of interest and costs, there are more than 100 putative class members defined below, and minimal diversity exists because a significant portion of putative class members are citizens of a state different from the citizenship of at least one Defendant.

28. This Court also has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 since this suit is brought under the laws of the United States.

29. This Court has supplemental jurisdiction over the remaining state law claims pursuant to 28 U.S.C. § 1367 because the state law claims form part of the same case or controversy under Article III of the United States Constitution.

30. This Court has general personal jurisdiction over UPMC because its principal place of business is within the Commonwealth. Additionally, this Court has specific personal jurisdiction over UPMC because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in the Commonwealth.

31. This Court has specific personal jurisdiction over Meta because a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in the Commonwealth. The privacy violations complained of herein resulted from Meta's intentional acts towards citizens of the Commonwealth while they were located within the Commonwealth. At all relevant times, Meta knew that its practices would directly result in the collection of information from Pennsylvania citizens.

32. Venue is proper in this District pursuant to 28 U.S.C. § 1391, as a substantial part of the events or omissions giving rise to the claim occurred within this District.

FACTUAL BACKGROUND

A. Meta and Advertising

33. Following the campus-wide infamy of FaceMash, an online "hot or not" game in which Harvard students compared two students' photos and voted on who was "hotter," Mark

Zuckerberg began writing code for a new website.[10] This new website would later come to be known as Facebook.

34. Facebook was launched in 2004 and reached its millionth registered user before the year's end. Merely four years later, Facebook had already reached the milestone of 100 million monthly active users.[11]

35. In 2007, Mark Zuckerberg announced the launch of Facebook Ads which, even then, gave advertisers "access to data on activity, fan demographics, ad performance and trends that better equip marketers to improve custom content on Facebook and adjust ad targeting."[12] Just three years later, third-party advertising accounted for 95% of Facebook's revenue.[13]

36. Advertising continues to account for the lion's share of Meta's revenue. In 2019, Meta brought in $69.66 billion in advertising revenue (98.5% of total revenue). In 2020, Meta brought in $84.17 billion in advertising revenue (97.9% of total revenue). In 2021, Meta brought in $117.93 billion in advertising revenue (97.5% of total revenue).[14]

---

[10] Katharine Kaplan, *Facemash Creator Survives Ad Board* (Nov. 19, 2003), https://www.thecrimson.com/article/2003/11/19/facemash-creator-survives-ad-board-the/.

[11] The Associated Press, *Number of Active Users at Facebook Over the Years*, Yahoo (Oct. 23, 2012), https://finance.yahoo.com/news/number-active-users-facebook-over-years-214600186--finance.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAANpSrN2n4sKRGr12jtBZzUHTDb2xEJOlCpRlshEwWGsyM4Iod1yAJWMKksxlai44WgP2LMk1642n4eWX7_6MtaBZWG1e5RvxW2ywyhrq7TnA3d4GQ2G3x9fTjnfjFnGroturfjOuXfN2uQpmCN580CwsKEQ9jsp8UB1NBQNQ2ly7.

[12] News, *Facebook Unveils Facebook Ads* (Nov. 6, 2007), https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/.

[13] Facebook Annual Report 2012 (Jan. 30, 2013), https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/FB_2012_10K.pdf.

[14] Meta Annual Report 2021 (Feb. 2, 2022), https://s21.q4cdn.com/399680738/files/doc_financials/2021/q4/FB-12.31.2021-Exhibit-99.1-Final.pdf.

37. Despite its financial success, Meta's targeted advertising has been the subject of numerous controversies.

38. For example, in June 2022, the Justice Department has entered into a settlement agreement resolving allegations that Meta engaged in discriminatory advertising in violation of the Fair Housing Act ("FHA"). Meta's "Lookalike Ad" service allowed housing advertisers to target users based on race, gender, and other FHA-protected characteristics. Meta has until December 2022 to make acceptable changes to its delivery of housing advertisements.[15]

39. Meta's targeted advertising has also been used to market antisemitic content to AI-identified antisemites,[16] to market diet programs to users with eating disorders,[17] to market weapons and armor to far-right militia groups ahead of the January 6th insurrection,[18] and to market alcohol, gambling, and tobacco to users between thirteen and seventeen years old.[19]

B. How Meta Pixel Works

40. In 2015, Meta Pixel was announced as a tool to refine Meta's targeted advertising.

---

[15] Settlement Agreement, *United States v. Meta Platforms, Inc.*, No. 1:22-cv-05187 (S.D.N.Y. 2022).

[16] Dani Deahl, *Facebook Restricts Ad Targeting After Anti-Semitism Controversy*, The Verge (Sep. 15, 2017), https://www.theverge.com/tech/2017/9/15/16313916/facebook-restricts-targeting-fields-anti-semitism-ads.

[17] Rae Nudson, *When Targeted Ads Feel a Little Too Targeted*, Vox (Apr. 9, 2020), https://www.vox.com/the-goods/2020/4/9/21204425/targeted-ads-fertility-eating-disorder-coronavirus.

[18] Mike Isaac, *Meta Plans to Remove Thousands of Sensitive Ad-Targeting Categories*, N.Y. Times (Nov. 9, 2021), https://www.nytimes.com/2021/11/09/technology/meta-facebook-ad-targeting.html.

[19] Kaveh Waddell, *Facebook Approved Alcohol and Gambling Ads Targeting Teens*, Consumer Reports, (July 27, 2021), https://www.consumerreports.org/advertising-marketing/facebook-approved-alcohol-gambling-tobacco-weight-loss-ads-targeting-teens-a1062200831/.

41. The Meta Pixel is a mechanism that loads JavaScript code which collects detailed and granular data for every interaction on a page.[20]

42. Once a third-party company, advertiser, or other entity sets up Meta Pixel on a website, the information collecting and sharing begins.

43. Importantly, Meta designed Meta Pixel such that Meta receives the information about a website user's actions contemporaneously with those actions. This means that as soon as a website user takes any action on a webpage that includes Meta Pixel, it redirects the user's communications to Meta while the exchange of the communication between the website users and the website is still occurring.

44. In response to congressional questioning in 2018, Meta stated that the Meta Pixel "provide[s] information about users' activities off Facebook—including information about their device, websites they visit, purchases they make, the ads they see, and how they use their services—whether or not they have a Facebook account or are logged into Facebook."[21]

45. Meta Pixel allows third parties to create a library which logs every time a website visitor takes an action (an "event") that the third party wants to track (a "conversion"). All of these tracked conversions are then stored so that the third party can analyze the data collected.[22]

---

[20] Surya Mattu, Angie Waller, Simon Fondrie-Teitler, & Micha Gorelick, *How We Built a Meta Pixel Inspector*, The Markup (Apr. 28, 2022), https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector.

[21] Facebook, Social Media Privacy, and the Use and Abuse of Data: Hearing Before the Comm. on Com., Sci., and Transp., 94 Cong. 115 (2018) (Post-Hearing Questions).

[22] *Meta for Developers*, Meta Pixel, https://developers.facebook.com/docs/meta-pixel/, (last visited Aug. 25, 2022).

46. There are currently more than six million websites using Meta Pixel.[23] On each of those websites, Meta Pixel collects and sends information to Meta via scripts running in a person's internet browser. That data is then delivered to Meta in "data packets" labeled with personally identifiable information ("PII"), including the user's IP address.

47. If a person is logged in to Facebook when they visit a website where Meta Pixel is installed, Meta is able to link collected data to specific Facebook accounts.

48. If a person is not logged in to Facebook at the time, Meta uses personal information that a user enters in form fields to match them to their Facebook and/or Instagram profile through a process called Advanced Matching. With this process, Meta collects emails, first and last names, phone numbers, birthdates, and addresses, then uses that information to connect event tracking data to a specific Facebook profile.

49. Even if a person does not have a Facebook account, has never registered for an account, has never so much as looked at a Facebook or Meta privacy policy, and has no intention to ever join any social media at all, Meta still collects data on that person. When asked by Congress about this maintenance of "shadow profiles" with data of nonusers of Facebook, Mark Zuckerberg responded, "[W]e collect data on people who have not signed up for Facebook for security purposes."[24]

---

[23] *Facebook Pixel Usage Statistics*, Built With, https://trends.builtwith.com/analytics/Facebook-Pixel, (last visited Agu. 25, 2022).

[24] Taylor Hatmaker, *Zuckerberg Denies Knowledge of Facebook Shadow Profiles*, TechCrunch (Apr. 11, 2018), https://techcrunch.com/2018/04/11/facebook-shadow-profiles-hearing-lujan-zuckerberg/.

50. A recent investigation by The Markup found that Meta Pixel is embedded on the websites of 33 of Newsweek's top 100 hospitals in the United States.[25] The Markup's investigation revealed that Meta Pixels installed on hospitals' websites have been collecting patients' sensitive health information—"including details about their medical conditions, prescriptions, and doctor's appointments"—and sending it to Meta.[26] This packet of data collected by Meta Pixel is connected to a patient's IP address, providing Meta with an intimate receipt of information that can be used in combination with other data to identify a specific individual or household.[27]

51. Most shocking, however, is that The Markup discovered that Meta Pixel is installed inside the password-protected patient portals of seven health systems.[28] The data Meta Pixel surreptitiously collected from patients' interactions with these patient portals included the names of their medications, descriptions of their allergies, and details about their upcoming doctor's appointments. [29]

52. The 33 hospitals found sending patients' sensitive health information to Meta collectively reported more than 26 million patient admissions and outpatient visits in 2020.[30] However, because The Markup's primary investigation was limited to Newsweek's top 100 hospitals, Meta's surreptitious harvesting of sensitive health information likely affects more patients and more hospitals than The Markup identified.

---

[25] Feathers et al., *supra* note 3.

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *Id.*

53. Indeed, a separate survey conducted jointly by The Markup and Reveal from The Center for Investigative Reporting, focused on crisis pregnancy centers, "found that at least 294 [centers] shared visitor information with Facebook," including highly sensitive information such as "whether a person was considering an abortion or looking to get a pregnancy test or emergency contraceptives."[31]

54. While Meta purports to "hash" patients' sensitive health information—obscuring them through a form of cryptography—before sending the information to Meta, the hashing does not prevent Meta from using that data. "Meta explicitly uses the hashed information to link pixel data to Facebook profiles."[32]

55. Moreover, Meta claims that "[i]t is against our policies for websites and apps to send sensitive information about people through our Business Tools," which includes its advertising technology, and its "system is designed to filter out potentially sensitive data it detects."[33] However, Meta told investigators from the New York Department of Financial Services that its filtering system was "not yet operating with complete accuracy," according to the department's February 2021 final report. [34] And more recently, The Markup and Reveal's joint

---

[31] Grace Oldham & Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients*, The Markup (June 15, 2022), https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients.

[32] Feathers et al., *supra* note 3.

[33] Oldham & Mehrotra, *supra* note 31.

[34] New York Department of Financial Services, *Report on Investigation of Facebook Inc. Data Privacy Concerns* (Feb. 18, 2021), https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf, at 11.

investigation found that Meta's sensitive health information filtering system did not block information about appointments a reporter requested with crisis pregnancy centers.[35]

56. Moreover, while Meta has an official, albeit ineffective, policy prohibiting the collection of sensitive health information, "it's unclear what if anything, the platform does to educate its advertising clients about the policy and proactively enforce it."[36]

57. Meta's failure to properly screen data Meta Pixel collects and prevent it from collecting sensitive health information, however, should come as no surprise. According to a leaked internal document, Meta engineers on the ad and business product team wrote: "We do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose.' And yet, this is exactly what regulators expect us to do, increasing our risk of mistakes and misrepresentation."[37] In other words, as explained by Johnny Ryan a privacy activist and senior fellow at the Irish Council for Civil Liberties, "[t]his document admits what we long suspected: that there is a data free-for-all inside Facebook and the company has no control whatsoever over the data it holds."[38]

---

[35] Oldham & Mehrotra, *supra* note 31.

[36] *Id.*

[37] Lorenzo Franceschi-Bicchierai, *Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document*, Vice (Apr. 26, 2022), https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes.

[38] *Id.*

58. David Holtzman, a health privacy consultant stated he is "deeply troubled by what [the] hospitals are doing with the capture [patient] data and the sharing of it."[39] He further indicated that the hospitals' use of the Meta Pixel "is quite likely a HIPAA violation."[40]

59. Plaintiff Smidga fell victim to Meta's unlawful harvesting and sharing of sensitive health information. Plaintiff is a patient of UPMC, has used UPMC's appointment scheduling page, and has been treated at one of UPMC's locations.

60. The Markup identified UPMC as one of 33 hospitals found to have the Meta Pixel collecting and sending patient appointment details to Meta.[41]

61. Plaintiff used the UPMC appointment scheduling page and entered sensitive personal and health information when scheduling appointments for medical treatment.

62. Unknown to Plaintiff, UPMC had allowed Meta Pixel to have access to the appointment scheduling page.

63. Meta utilized this access to surreptitiously gather Plaintiff's sensitive personal and health information.

64. After entering this information on the appointment scheduling page and receiving medical treatment at one of UPMC's locations, Plaintiff started receiving advertisements on her Facebook related to her the medical symptoms she complained of when scheduling an appointment and the medical treatment she subsequently received.

65. As such, Meta and UPMC have used and published Plaintiff's sensitive health information for their own profit.

---

[39] Feathers, et al., *supra* note 3.

[40] *Id.*

[41] *Id.*

C. Plaintiff and Class Members Have a Reasonable Expectation of Privacy Regarding Their Data, Specifically Regarding Their Sensitive Health Information

66. Plaintiff and Class Members have a reasonable expectation of privacy in their data communicated to UPMC, including personal information and sensitive health information.

67. As one law professor from the University of Michigan put it, the Meta Pixel's surreptitious collection of sensitive health information "is an extreme example of how far the tentacles of Big Tech reach into what we think of as protected data space."[42]

68. Another law professor characterized Defendants' actions as "totally outside of the expectations of what patients think the health privacy laws are doing for them."[43]

69. UPMC is an entity covered under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1302d, *et seq*. ("HIPAA"), which sets minimum federal standards for privacy and security of protected health information ("PHI").

70. Under 45 C.F.R. § 160.103, HIPAA defines "protected health information" or PHI as "individually identifiable health information" that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium."

71. Under C.F.R. § 160.103, HIPAA defines "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual" that is (1) "created or received by a health care provider;" (2)"[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an

---

[42] Feathers et al., *supra* note 3.

[43] *Id.*

individual;" and (3) either (a) identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual."

72. HIPAA requires UPMC to: (a) ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits; (b) identify and protect against reasonably anticipated threats to the security or integrity of the electronic PHI; (c) protect against reasonably anticipated, impermissible uses, or disclosures of the PHI; and (d) ensure compliance by its workforce to satisfy HIPAA's security requirements. 45 CFR § 164.102, *et. seq*.

73. HIPAA further prohibits a healthcare provider from disclosing PHI with third parties, such as Meta, except where an individual has expressly consented in advance to the disclosure or under certain HIPAA-compliant contracts. 45 C.F.R. §§ 164.502 & 164.508.

74. Upon information and belief, neither UPMC nor Meta obtained Plaintiff's and Class members' express consent to share their sensitive health information nor have UPMC or Meta entered into a HIPAA-compliant contract that would permit such sharing.

75. Given the application of HIPAA to UPMC, and that Plaintiff and Class members must entrust their sensitive health information to UPMC in order to receive care, Plaintiff and members of the Class had a reasonable expectation of privacy in their sensitive health information provided to UPMC.

D. Plaintiff and Class Members Do Not Consent to Defendants' Collection or Use of Their Data

76. Plaintiff and Class members have no idea Meta collects and uses their sensitive health information when they interact with a hospital's appointment scheduling page because Meta Pixel is seamlessly incorporated into the background, as Meta Pixel is an invisible 1x1 tracking pixel.

77. For instance, when Plaintiff was on UPMC's appointment scheduling page, there was no indication that Meta Pixel was embedded or that it would collect her sensitive health information.

78. UPMC's own "Notice of Privacy Practices" and "Website Terms of Use" only make vague references to marketing cookies that collect a patient's health information to promote its own products and services, not sharing such information with Meta for Meta's financial gain.

79. Moreover, while Meta purports to maintain a "Data Policy" that vaguely states under a buried heading "Information from partners" that its "partners provide information about your activities" including "websites you visit," Plaintiff and Class members would not have a reason to visit or have read Meta's website, let alone its Data Policy, when scheduling appointments or inputting medical information intended their medical providers such as UPMC.

80. Even if Plaintiff did encounter Meta's Data Policy stating in vague terms that Meta may receive information from "websites you visit," this undescriptive provision would not be understood by any reasonable user to mean that Meta collects and uses sensitive health information provided to UPMC to receive medical services.

81. Indeed, the collection of Plaintiff's and Class members' sensitive health information is inconsistent with the remaining provisions of Meta's Data Policy. Meta requires its purported "Partners" "to have the right to collect, use, and share [user's] information before giving it to [Meta]."

82. But UPMC does not have an unlimited right to share Plaintiff's or Class members' data. UPMC is a covered entity under HIPAA, and HIPAA protects all electronically protected health information a covered entity like UPMC "creates, receives, maintains, or transmits" in electronic form. 45 C.F.R. § 160.103.

83. Further, HIPAA does not permit the use or disclosure of sensitive health information to Meta for use in targeted advertising without Plaintiff and the Class members' express consent unless UPMC and Meta entered into a HIPAA-approved contract. 45 C.F.R. §§ 164.502 & 164.508.

84. Upon information and belief, however, neither UPMC nor Meta obtained Plaintiff's and Class members' express consent to share their sensitive health information nor have UPMC or Meta entered into a HIPAA-compliant contract that would permit such sharing.

85. Thus, Defendants did not obtain consent to collect, use, and store Plaintiff's and Class members' sensitive health information.

E. Defendants Were Aware that Plaintiff's Data Included Sensitive Health Information

86. Defendants were well aware that by placing Meta Pixel on UPMC's appointment scheduling page, it would result in the disclosure and use of Plaintiff's and Class members' sensitive health information.

87. On November 9, 2021, Facebook announced that it was removing the ability to target users on "topics people may perceive as sensitive, such as options referencing causes, organizations, or public figures that relate to health[.]"[44]

88. But despite this publicity stunt, Meta did not change the most insidious types of targeting based on health—those marketing campaigns from medical providers that disclose patient identities and their individually identifiable health information to Facebook for the purpose of targeted marketing based on their communications with their medical providers.

---

[44] *Removing Certain Ad Targeting Options and Expanding our Ad Controls*, Meta (Nov. 9, 2021), https://www.facebook.com/business/news/removing-certain-ad-targeting-options-and-expanding-our-ad-controls.

89. By design of Meta Pixel, *i.e.*, sending all interactions on a website to Meta, UPMC was well aware that their patients' sensitive health information would be sent to Meta when they made appointments or otherwise interacted with the website.

90. One patient portal company, Epic Systems—the software company behind MyChart that provides access to medical records to hospitals—has "specifically recommended heightened caution around the use of custom analytics scripts."[45] Despite this, UPMC chose to embed the Meta Pixel into the appointment scheduling page.

91. Likewise, Meta was acutely aware that by embedding Meta Pixel in hospitals' patient portals, it would enable the collection of patients' sensitive health information.

92. For instance, the FTC recently reached a settlement with Flo Health, Inc., arising from allegations that the fertility-tracking app was sharing sensitive health information from millions of its users with marketing and analytics firms, including Meta and Google.[46]

93. The New York State Department of Financial Services reached a similar conclusion in February of 2021, finding that Meta collected sensitive health information in violation of its own policies. "Facebook acknowledged to DFS that, until DFS commenced its investigation, Facebook routinely obtained sensitive data from app developers, particularly in the area of health-related information, contrary to its own policies."[47] "The information provided by Facebook has

---

[45] Feathers et al., *supra* note 3.

[46] *FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others,* FTC (June 22, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.

[47] New York Department of Financial Services, *Report on Investigation of Facebook Inc. Data Privacy Concerns* (Feb. 18, 2021), https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_202.10218.pdf, at 7.

made it clear that Facebook's internal controls on this issue have been very limited and were not effective at enforcing Facebook's policy or preventing the receipt of sensitive data."[48] "Merely stating a rule, however, has little meaning if the rule is not enforced, and the unfortunate fact is that Facebook does little to track whether app developers are violating this rule and takes no real action against developers that do."[49]

94. The Markup and Reveal's own investigation also revealed that Facebook continues to ingest data from webpages with sensitive health information, including the URLS with the most obvious sexual health information—"post-abortion," "i-think-im-pregnant," and "abortion-pill."[50]

95. Despite Meta knowing it was receiving sensitive health information through Meta Pixel when enabled on apps and websites that provide health-related services—and knowing that its own "polices" are woefully insufficient to screen medical information from being collected—Meta still enabled Meta Pixel on UPMC's and other hospitals websites and patient portals and received sensitive health information well through 2022.

F. Plaintiff and Class Members Suffered Harm as a Result of the Illicit Disclosure of Their Sensitive Health Information.

96. Meta has built its business around the collection of personal data because "data is widely considered to be among the world's most valuable resources" based on how much potential revenue and business value it can provide, becoming "a valuable commodity, similar to commodities like oil and gold."[51]

---

[48] *Id.* at 7–8.

[49] *Id.* at 16.

[50] Oldham & Mehrotra, *supra* note 31.

[51] Vijay Cherukuri, *Data: The most Valuable Commodity for Business*, KD Nuggets (Mar. 1, 2022), https://www.kdnuggets.com/2022/03/data-valuable-commodity-businesses.html.

97. The FTC has identified data collected about a person's precise location and information about their health as the most sensitive categories of data collected. Standing alone, these data points "pose an incalculable risk to personal privacy" but when technology companies collect the data, combine it, and sell or monetize it, this amounts to an "unprecedented intrusion" and creates "a new frontier of potential harms to consumers."[52]

98. For example, the FTC recently reached a settlement with Flo Health, alleging the company shares sensitive health information about women collected from its period and fertility tracking app with Google and Meta, despite promising to keep this information private. FTC warns that the misuse use of such health information, including reproductive health data, exposes consumers to significant harm because: (1) criminals can use the health data to facilitate phishing scams or commit identity theft; (2) stalkers or other criminals can use the data to inflict physical and emotional injury; and (3) the exposure of health information and medical conditions can subject people to discrimination, stigma, mental, anguish, and other serious harms.[53]

99. As Chris Bowen, The Chief Privacy and Security Officer for ClearData, explained, health information is so valuable because "[y]ou can build [an] entire human persona around a health record. You can create or seek medical treatment, abuse drugs, or get prescriptions."[54] This

---

[52] Kristen Cohen, Location, health, and other sensitive information: FTC committed to fully enforcing the law against illegal use and sharing of highly sensitive data, FTC (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal-use.

[53] *Id.*

[54] Will Maddox, Why Medical Data is 50 Times More Valuable Than a Credit Card, DMagazine (Oct. 15, 2019), https://www.dmagazine.com/healthcare-business/2019/10/why-medical-data-is-50-times-more-valuable-than-a-credit-card/.

is part of the reason why healthcare data may be valued at up to $250 per record on the black market.[55]

100. However, data is not just valuable to criminals. It is common knowledge that there is an economic market for consumers' personal data, including the sensitive health information Defendants collected from Plaintiff and Class Members.

101. Healthcare providers, such as UPMC "sit on treasure troves: a stockpile of patient health data stored as electronic medical records."[56] These "files show what people are sick with, how they were treated, and what happened next."[57] Taken together, they're hugely valuable resources for medical discovery."[58] When healthcare providers de-identify the records, *i.e.*, remove identifying information such as names, locations, and phone numbers, healthcare providers can sell the data to partners for research.

102. Unsurprisingly, healthcare groups have taken advantage of de-identifying medical records. The Mayo Clinic in Rochester, Minnesota is working with a startup to develop algorithms to diagnose and manage conditions based on health data.[59] Fourteen U.S. healthcare systems

---

[55] Tori Tyalor, Hackers, *Breaches, and the Value of Healthcare Data*, SecureLink (June 30, 2021), https://www.securelink.com/blog/healthcare-data-new-prize-hackers.

[56] Nicole Wetsman, *Hospitals are selling treasures troves of medical data – what could go wrong?*, The Verge (June 23, 2021), https://www.theverge.com/2021/6/23/22547397/medical-records-health-data-hospitals-research.

[57] *Id.*

[58] *Id.*

[59] *Id.*

formed a company to aggregate and sell de-identified data.[60] And one hospital chain even researched an agreement with Google to use patient data to develop healthcare algorithms.[61]

103. Given the monetary values of sensitive health information, Defendants have deprived Plaintiff and the Class members of the economic value of their sensitive health information by acquiring such data without providing proper consideration for Plaintiff's and Class members' property.

TOLLING

104. Defendants seamlessly incorporated Meta Pixel into websites, providing no indication to users that they were interacting with a website with Meta Pixel enabled.

105. Defendants had exclusive knowledge that UPMC's websites incorporated Meta Pixel yet failed to disclose that by interacting with the Meta Pixel-enabled websites that Plaintiff's and Class members sensitive health information would be collected, used, and stored by Meta.

106. Plaintiff and Class Members could not with due diligence have discovered the full scope of Defendants' conduct, including because there were no disclosures or other indication that they were interacting with Meta-Pixel enabled websites.

107. The earliest Plaintiff and Class members, acting with due diligence, could have reasonably discovered this conduct would have been on June 16, 2022, following the release of The Markup's investigation.

---

[60] *Id.*

[61] Nicole Westman, *Google to use patient data to develop healthcare algorithms for hospital chain*, The Verge (May 26, 2021), https://www.theverge.com/2021/5/26/22454817/google-hca-patient-data-healthcare-algorithms.

CLASS ACTION ALLEGATIONS

108. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 individually and on behalf of the following Classes:

> **Nationwide Class**: All natural persons in the United States whose personal information was collected through Meta Pixel.
>
> **Pennsylvania Subclass**: All natural persons in the Commonwealth of Pennsylvania whose personal information was collected through Meta Pixel.

109. Excluded from the classes are: (1) any Judge or Magistrate presiding over this action and any members of their immediate families; (2) the Defendants, Defendants' subsidiaries, affiliates, parents, successors, predecessors, and any entity in which the Defendants or their parents have a controlling interest and their current or former employees, officers, and directors; and (3) Plaintiff's counsel and Defendants' counsel.

110. **Numerosity**: The exact number of members of the Class is unknown and unavailable to Plaintiff at this time, but individual joinder in this case is impracticable. The Classes likely consists of millions of individuals, and the members can be identified through Meta's records.

111. **Predominant Common Questions**: The Classes' claims present common questions of law and fact, and those questions predominate over any questions that may affect individual Class members. Common questions for the Classes include, but are not limited to, the following:

a. Whether Plaintiff and Class Members had a reasonable expectation of privacy in their sensitive health information communicated to their healthcare providers;

b. Whether Meta Pixel is designed to send individually identifiable information to Meta;

c. Whether Meta and UPMC violated Plaintiff's and Class Members' privacy rights;

d. Whether Meta's acquisition of the contents of electronic communications between patients and their medical providers occurred contemporaneous to their making;

e. Whether Meta acquired the contents of electronic communications between patients and their medical providers without Plaintiff's and Class Members' consent;

f. Whether Meta's actions violated the Pennsylvania Wiretap Act,18 Pa. Cons. Stat. § 5701, *et seq*.;

g. Whether Meta's actions violated the Federal Wiretap Act, 18 U.S.C. §§ 2510, *et seq*.;

h. Whether Plaintiff and the Class Members are entitled to equitable relief; and

i. Whether Plaintiff and the Class Members are entitled to actual, statutory, punitive, or other forms of damages, and other monetary relief.

112. **Typicality**: Plaintiff's claims are typical of the claims of the other members of the Classes. The claims of Plaintiff and the members of the Classes arise from the same conduct by Defendants and are based on the same legal theories.

113. **Adequate Representation**: Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Classes. Plaintiff has retained counsel competent and experienced in complex litigation and class actions, including litigations to remedy privacy violations. Plaintiff has no interest that is antagonistic to the interests of the Classes, and Defendants have no defenses unique to any Plaintiff. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the members of the Classes, and they have the

resources to do so. Neither Plaintiff nor her counsel have any interest adverse to the interests of the other members of the Classes.

114. **Substantial Benefits**: This class action is appropriate for certification because class proceedings are superior to other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Classes is impracticable. This proposed class action presents fewer management difficulties than individual litigation, and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court. Class treatment will create economies of time, effort, and expense and promote uniform decision-making.

115. Plaintiff reserves the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

CAUSES OF ACTION

COUNT I
Breach of Fiduciary Duty
(Plaintiff On Behalf of Pennsylvania Subclass)
Against UPMC

116. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

117. Plaintiff brings this claim individually and on behalf of the Pennsylvania Subclass.

118. Plaintiff and Class members have an interest, both equitable and legal, in their sensitive health information that was conveyed to and collected by UPMC, and ultimately disclosed to Meta without Plaintiff's or the Class members' consent.

119. As a healthcare provider, UPMC has a fiduciary relationship to its patients, like Plaintiff and the Class Members.

120. Because of that fiduciary and special relationship, UPMC was provided with and stored Plaintiff's and Class members' sensitive health information, and owes them, at a minimum a duty of confidence and confidentiality.

121. UPMC owed a fiduciary duty under common law to Plaintiff and Class Members to exercise the utmost care in obtaining, retaining, safeguarding, and protecting their sensitive health information in its possession from being disclosed to, accessed by, and misused by unauthorized persons.

122. UPMC breach the duties owed to Plaintiff and Class members by installing Meta Pixel on the appointment scheduling page and disclosing Plaintiff and Class members' sensitive health information without their consent to Meta for financial gain.

123. But for UPMC's wrongful breach of its duties owed to Plaintiff and Class members, their sensitive health information would not have been disclosed.

124. As a direct result of UPMC's breaches of its fiduciary duty and duty of confidentiality, Plaintiff and Class Members have suffered injuries, including but not limited to:

a. Damages that will reasonably compensate Plaintiff and Class members from the harm to their privacy interests in their sensitive health information;

b. Damages that will reasonably compensate Plaintiff and Class members for the breach of their confidences and the erosion of their confidential relationship between patient and healthcare provider;

c. Emotional distress from the unauthorized disclosure of their sensitive health information for financial gain; and

d. Disgorgement of any profits made as a result of UPMC's disclosure of Plaintiff's and Class members' sensitive health information.

125. As a direct and proximate result of UPMC's breach of its fiduciary duty, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT II
Violation of Common Law Invasion of Privacy – Intrusion Upon Seclusion
(Plaintiff On Behalf of Pennsylvania Subclass)
Against UPMC

126. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

127. Plaintiff brings this claim individually and on behalf of the Pennsylvania Subclass.

128. Pennsylvania common law recognizes the tort of invasion of privacy. The right to privacy is also embodied in multiple sections of the Pennsylvania constitution.

129. Plaintiff and Class members had a reasonable expectation of privacy in their sensitive health information. Plaintiff and Class members did not consent to, authorize, or know about UPMC's intrusion at the time it occurred. Plaintiff and Class members never agreed that UPMC could disclose their sensitive health information to third parties, including sensitive health information. Plaintiffs intended their sensitive health information to stay private from third parties without their consent and UPMC represented that their sensitive health information would stay private and confidential.

130. Plaintiff and Class members had an interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

131. UPMC intentionally intruded upon Plaintiff's and Class Members' private life, seclusion, or solitude, without consent.

132. UPMC's conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy because Plaintiff's and Class Members' sensitive health information is private and was intended to remain private and confidential.

133. Plaintiff and Class members were harmed by UPMC's wrongful conduct as UPMC's conduct has caused Plaintiff and the Class psychological and emotional anguish, distress, and suffering arising from their loss of privacy and confidentiality of their sensitive health information.

134. As a direct and proximate result of UPMC's conduct, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT III
Violation of Common Law Invasion of Privacy – Intrusion Upon Seclusion
(Plaintiff On Behalf of Pennsylvania Subclass)
Against Meta

135. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

136. Plaintiff brings this claim individually and on behalf of the Pennsylvania Subclass.

137. Pennsylvania common law recognizes the tort of invasion of privacy. The right to privacy is also embodied in multiple sections of the Pennsylvania constitution.

138. Plaintiff and Class members had a reasonable expectation of privacy in their sensitive health information. Plaintiff and Class members did not consent to, authorize, or know about Meta's intrusion at the time it occurred. Plaintiff and Class members never agreed that Meta could collect or disclose their sensitive health information.

139. Plaintiff and Class members had an interest in precluding the dissemination and/or misuse of their information and communications and in conducting their personal activities

without intrusion or interference, including the right to not have their personal information intercepted and utilized for business gain.

140. Meta intentionally intruded on Plaintiff's and Class members' private life, seclusion, or solitude, without consent.

141. Meta's conduct is highly objectionable to a reasonable person and constitutes an egregious breach of the social norms underlying the right to privacy because Plaintiff's and Class Members' sensitive health information is private and was intended to remain private and confidential.

142. Plaintiff and Class members were harmed by Meta's wrongful conduct as Meta's conduct has caused Plaintiff and the Class psychological and emotional anguish, distress, and suffering arising from their loss of privacy and confidentiality of their sensitive health information.

143. As a direct and proximate result of Meta's conduct, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT IV
Violation of Pennsylvania Wiretap Act
18 Pa. Cons. Stat. § 5701, *et seq*.
(Plaintiff On Behalf of Pennsylvania Subclass)
Against Meta

144. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

145. Plaintiff brings this claim individually and on behalf of the Pennsylvania Subclass.

146. The Pennsylvania Wiretap Act ("WESCA") prohibits (1) the interception or procurement of another to intercept any wire, electronic, or oral communication; (2) the intentional disclosure of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral

communication; and (3) the intentional use of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication. 18 Pa. Cons. Stat. § 5703.

147. Any person who intercepts, discloses, or uses or procures any other person to intercept, disclose, or use, a wire, electronic, or oral communication in violation of WESCA is subject to a civil action for (1) actual damages, not less than liquidated damages computed at the rate of $100/day for each violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred. 18 Pa. Cons. Stat. § 5725(a).

148. "Intercept" is defined as any "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." 18 Pa. Cons. Stat. § 5702.

149. "Contents" is defined as "used with respect to any wire, electronic or oral communication, is any information concerning the substance, purport, or meaning of that communication." 18 Pa. Cons. Stat. § 5702.

150. "Person" is defined as "any individual, partnership, association, joint stock company, trust or corporation." 18 Pa. Cons. Stat. § 5702.

151. "Electronic Communication" is defined as "[a]ny transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system." 18 Pa. Cons. Stat. § 5702.

152. Meta is a person for purposes of WESCA because it is a corporation.

153. Meta Pixel is a "device" used for the "acquisition of the contents of any wire, electronic, or oral communication" within the meaning of WESCA.

154. Plaintiff's and Class members' sensitive health information which was intercepted by Meta through Meta Pixel are the "contents" of "electronic communication[s]" within the meaning of WESCA.

155. Plaintiff's and Class members' electronic communications were intercepted contemporaneously during transmission, without their consent and for the unlawful and/or wrongful purpose of monetizing their private information, including by using their sensitive health information to develop marketing and advertisement strategies.

156. Interception of Plaintiff's and Class members' private and confidential electronic communications without their consent occurs whenever users engage with the UPMC appointment scheduling page. Meta is not party to these communications

157. Plaintiff and the Class members had a justified expectation under the circumstances that their electronic communications would not be intercepted.

158. Meta had no right to intercept, collect, and disclose Plaintiff's and the Class members' sensitive health information. Neither Plaintiff nor the Class consented to Defendants' interception, disclosure, and/or use of their sensitive health information in their electronic communications with the UPMC appointment scheduling page. Nor could they. Meta and UPMC never sought to or did obtain Plaintiff's or the Class members' consent.

159. Meta's conduct has needlessly harmed the Plaintiff and the Class by disclosing intimately personal facts and data in the form of their sensitive health information. This disclosure and loss of privacy and confidentiality has caused the Plaintiff and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

160. Pursuant to 18 Pa. Cons. Stat. 5725(a), Plaintiff and the Class members seek (1) actual damages, not less than liquidated damages computed at the rate of $100/day for each

violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred.

COUNT V
Violation of Pennsylvania Wiretap Act
18 Pa. Cons. Stat. § 5701, *et seq*.
(Plaintiff On Behalf of Pennsylvania Subclass)
Against UPMC

161. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

162. Plaintiff brings this claim individually and on behalf of the Pennsylvania Subclass.

163. WESCA prohibits (1) the interception or procurement of another to intercept any wire, electronic, or oral communication; (2) the intentional disclosure of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication; and (3) the intentional use of the contents of any wire, electronic, or oral communication that the discloser knew or should have known was obtained through the interception of a wire, electronic, or oral communication. 18 Pa. Cons. Stat. § 5703.

164. Any person who intercepts, discloses, or uses or procures any other person to intercept, disclose, or use, a wire, electronic, or oral communication in violation of WESCA is subject to a civil action for (1) actual damages, not less than liquidated damages computed at the rate of $100/day for each violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred. 18 Pa. Cons. Stat. § 5725(a).

165. "Intercept" is defined as any "[a]ural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device." 18 Pa. Cons. Stat. § 5702.

166. "Contents" is defined as "used with respect to any wire, electronic or oral communication, is any information concerning the substance, purport, or meaning of that communication." 18 Pa. Cons. Stat. § 5702.

167. "Person" is defined as "any individual, partnership, association, joint stock company, trust or corporation." 18 Pa. Cons. Stat. § 5702.

168. "Electronic Communication" is defined as "[a]ny transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system." 18 Pa. Cons. Stat. § 5702.

169. UPMC is a person for purposes of WESCA because it is a corporation.

170. Meta Pixel is a "device" used for the "acquisition of the contents of any wire, electronic, or oral communication" within the meaning of WESCA.

171. Plaintiff's and Class members' sensitive health information which was intercepted by UPMC through Meta Pixel are the "contents" of "electronic communication[s]" within the meaning of WESCA.

172. UPMC procured Meta to automatically and secretly spy on, and intercept its patients' sensitive health information communicated through the UPMC appointment scheduling page in real time.

173. To facilitate this wiretap, UPMC installed the Meta Pixel on its website and the UPMC appointment scheduling page.

174. Upon information and belief, UPMC knew by embedding the Meta Pixel on its website and appointment scheduling page, this would disclose to Meta, UPMC's patients' sensitive health information communicated through the appointment scheduling page.

175. Upon information and belief, UPMC intentional used its patients' sensitive health information obtained through the Meta Pixel, to develop marketing and advertisement strategies direct towards its patients.

176. Interception of Plaintiff's and Class members' private and confidential electronic communications without their consent occurs whenever users engage with the UPMC appointment scheduling page.

177. Plaintiff and the Class members had a justified expectation under the circumstances that their electronic communications would not be intercepted, especially where UPMC is a HIPAA covered entity to whom patients entrust their sensitive health information in order to receive medical care from UPMC.

178. UPMC had no right to intercept, collect, and disclose the Plaintiff's and the Class members' sensitive health information. Neither Plaintiff nor the Class consented to Defendants' interception, disclosure, and/or use of their sensitive health information in their electronic communications with the UPMC appointment scheduling page. Nor could they. Meta and UPMC never sought to or did obtain Plaintiff's or the Class members' consent.

179. UPMC's conduct has needlessly harmed Plaintiff and the Class by disclosing intimately personal facts and data in the form of their sensitive health information. This disclosure and loss of privacy and confidentiality has caused the Plaintiff and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

180. Pursuant to 18 Pa. Cons. Stat. 5725(a), Plaintiff and the Class members seek (1) actual damages, not less than liquidated damages computed at the rate of $100/day for each violation or $1,000, whichever is higher; (2) punitive damages; and (3) reasonable attorneys' fees and other litigation costs incurred.

COUNT VI
Violation of the Federal Wiretap Act
18 U.S.C. §§ 2510, *et seq*.
(On Behalf of Nationwide Class)
Against Meta

181. Plaintiff incorporates the preceding paragraphs as if fully set forth herein.

182. Plaintiff brings this claim individually and on behalf of the Nationwide Class

183. The Federal Wiretap Act, 18 U.S.C. §§ 2510 *et seq*. ("FWA"), prohibits the interception of any wire, oral, or electronic communications without the consent of at least one authorized party to the communication. The statute confers a civil cause of action on "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

184. "Intercept" is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

185. "Contents" is defined as "includ[ing] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

186. "Person" is defined as "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6).

187. "Electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce . . . ." 18 U.S.C. § 2510(12).

188. Meta is a person for purposes of FWA because it is a corporation.

189. Meta Pixel is a "device" used for the "acquisition of the contents of any wire, electronic, or oral communication" device or apparatus" that is "used to intercept a wire, oral, or electronic communication" within the meaning of FWA.

190. Plaintiff's and Class members' sensitive health information which was intercepted by Defendants through the Meta Pixel are the "contents" of "electronic communication[s]" within the meaning of FWA.

191. Plaintiff's and Class members' electronic communications were intercepted during transmission, without their consent and for the unlawful and/or wrongful purpose of monetizing their private information, including by using their sensitive health information to develop marketing and advertisement strategies.

192. Interception of Plaintiff's and Class members' private and confidential electronic communications without their consent occurs whenever users engage with the UPMC appointment scheduling page. Meta is not party to these communications

193. Plaintiff and the putative class members had a justified expectation under the circumstances that their electronic communications would not be intercepted.

194. Meta had no right to intercept, collect, and disclose the Plaintiff's and the Class members' sensitive health information. Neither Plaintiff nor the Class consented to Defendants' interception, disclosure, and/or use of their sensitive health information in their electronic communications with the UPMC appointment scheduling page. Nor could they. Meta and UPMC never sought to or did obtain Plaintiff's or the Class members' consent.

195. Meta's conduct has needlessly harmed Plaintiff and the Class by disclosing intimately personal facts and data in the form of their sensitive health information. This disclosure

and loss of privacy and confidentiality has caused Plaintiff and the Class to experience mental anguish, emotional distress, worry, fear, and other harms.

196. Pursuant to 18 U.S.C. § 2520, Plaintiff and Class Members have been damaged by the interception, disclosure, and/or use of their communications in violation of the FWA and are entitled to: (1) appropriate equitable or declaratory relief; (2) actual damages, not less than liquidated damages computed at the rate of $100/day or $10,000, whichever is greater; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of herself and the proposed Classes respectfully requests that the Court enter an order:

A. Certifying the Classes and appointing Plaintiff as the Classes' representative;

B. Appoint the law firm Lynch Carpenter, LLP as class counsel;

C. Finding that Defendants' conduct was unlawful, as alleged herein;

D. Awarding declaratory relief against Defendants;

E. Awarding such injunctive and other equitable relief as the Court deems just and proper;

F. Awarding Plaintiff and the Class members statutory, actual, compensatory, consequential, punitive, and nominal damages, as well as restitution and/or disgorgement of profits unlawfully obtained;

G. Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

H. Awarding Plaintiff and the Class members reasonable attorneys' fees, costs, and expenses; and

I. Granting such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of herself and the Classes, demands a trial by jury of any and all issues in this action so triable of right.

Dated: August 25, 2022

Respectfully submitted,

/s/ Gary F. Lynch

Gary F. Lynch
Jamisen A. Etzel
Nicholas A. Colella
Patrick D. Donathen
LYNCH CARPENTER, LLP
1133 Penn Ave., 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
gary@lcllp.com
jamisen@lcllp.com
nickc@lcllp.com
patrick@lcllp.com

Counsel for Plaintiff